Application Development Domain

Description

The Application Development & Management Domain defines roles, development methodologies, technology standards, and technologies that define how applications are designed and how they cooperate. It defines how those applications are documented and maintained. The Application Development & Management Domain provides criteria, approved methodologies, and technologies that optimize the use and reuse of application components. The domain includes strategies for the retention of legacy knowledge and the phase out or upgrade of legacy systems.

Some examples of subject areas include but are not limited to:

- Methodologies
- Business Rules
- Development Tools
- Commercial Products
- Database Interface
- Middleware Interface
- N-Tiered Development
- Rapid Application Development (RAD)
- Joint Application Development (JAD)
- Components
- Repository (code reuse)
- Asynchronous Processing

Software engineering tools include:
Integrated Computer Aided Software Engineering (ICASE),
Object Oriented Programming (OOP),
Requirements Management and Tracking, Automated Software Testing Tools
Artificial Intelligence

Purpose

The Application Development & Management domain standardizes the methodology, approach, and technology components used in application development. The domain has relationships with but does **not** include database applications and middleware or their associated platforms and operating systems. The Application Development & Management domain does not include the security and privacy aspects associated with deployment of these technologies. The Middleware Architecture, Platform Architecture, Data Management Architecture, Security Architecture, and Privacy domains need to be referenced for guidance on those aspects associated with implementation of these technologies.

The Application Development & Management domain promotes common presentation standards to facilitate rapid training and implementation of new applications and functions. Good application architecture enables a high level of system integration, reuse of components, and rapid deployment of applications in response to changing business requirements.

The Application Development & Management domain standardizes the approach to application development. This standardization provides a cost effective approach to application development and minimizes training and retraining requirements. The capability to retain staff will be increased by the simplification of staff retraining and a more effective investment of available project funding.

- Deploy applications systems that are (business) event-driven.
- Application systems should be re-engineer to be “highly granular” and “loosely coupled”.
- Applications systems employ reusable components using an n-tier model.
- Application systems should share reusable components across the enterprise
- Leverage the data warehouse to accelerate decision-making and reduce the development burden.

Principles

❑ A business process analysis and review must always accompany automation efforts. Before automating business processes, a demonstrated attempt must be made to eliminate unnecessary processes and to simplify those remaining.

❑ The order of preference for solution delivery will be to reuse existing, purchase new and then build.

❑ Application programs, whether purchased or developed internally, will be architected with separation of presentation logic, business logic and data access in order to provide modular, reusable functionality.

❑ New applications will be modular and independent (“atomic”) in nature. They will access common data, use common services and have only inherently essential dependence on other applications (e.g. for provision of up-to-date data).

❑ New applications will use defined and documented standards-based programming interfaces.

❑ Long-term plans will be considered when implementing new systems to avoid obsolescence. Agency IT plans need to develop strategies for the removal of non-strategic or retired technologies.

❑ Vendor neutral standards should be applied to reduce effort required for system integration. Exceptions should be negotiated and mitigated.

❑ Application configuration decisions should be based on N-tiered technology

❑ Hardware and software should comply with industry standards for remote control and monitoring.

❑ Applications should present a consistent user interface that is adaptable to a particular user's requirement.

Standards

ANSI/IEEE 1209-1992 (Evaluation and Selection of ICASE Tools) ICASE/Software development environment

NIST FIPS PUB 160 (C) Programming languages - C and C++

NIST FIPS PUB 21-4 (COBOL) Programming languages – COBOL

ISO 1539:1990 (FORTRAN-90) Programming languages – FORTRAN

NIST FIPS PUB 69-1 (FORTRAN-77) Programming languages – FORTRAN

NIST FIPS PUB 125-1 (MUMPS)Programming languages – MUMPS

ANSI/IEEE 1016-1987 (Recommended Practice for Software Design Descriptions) Software design

ANSI/IEEE 1016.1-1993 (Guide for Software Design Descriptions) Software design

Technologies

The increasing failure of traditional software development methods is producing fundamentally new techniques for the execution of IT projects.

- Buy vs. Build
  - Turnkey or "80%" tailored COTS solutions
- Component Based Development
  - Planned Reuse & COTS subcomponents
  - Object-Oriented Methods and Technologies
- "Sledgehammer" Engineering
  - Over specify hardware rather than spending engineering labor

Asset Management Domain

Description

Asset management defines the policies, procedures, standards and systems required for the tracking and reporting of assets owned by the government entity including: software licensing, metering, asset tracking, asset replacement, asset retirement, software distribution, and inventory. Keeping track of who has what, where it is located, and how it is configured is a considerable task. Other tasks associated with asset management include, but are not limited to the tracking of service level agreements, capacity management, cost management, and personnel skills inventory.

Purpose

Tracking assets in a central repository will allow for increased potential for predicting future problems, allowing IT staff to analyze data and have the Help Desk act in a more productive mode of operation Improved forecasting of equipment upgrades will better enable staff equipment needs to be met, thus improving productivity. Reliable response to inquiries regarding assets will improve customer satisfaction. Automating inventory functions will allow personnel to be reallocated to more business critical duties.

The technical skills of the staff are also valuable assets and technical skill retention has to be an enterprise goal Resource pools and knowledge sharing will be encouraged.

Principles

❑ Owners will be identified for all IT assets – applications, data and technologies.

❑ Owners will be responsible for the management, administration and usage of these assets.

Standards

Technologies

Emerging Standard	Current Standard	Twilight Standard
• Full range of auto-discovery capabilities (desktops, servers, hosts, operating systems, network infrastructure) • Integration with other systems (e.g. network management, Help Desk)	• Computerized databases and spreadsheets • Some asset discovery capability • Limited integration with other systems	• Manual processes

Business Continuity Domain

Description

The Business Continuity domain defines the roles, standards, policies, and technologies for disaster recovery and restoring the enterprise to full functionality.

Purpose

Contingency planning is necessary to ensure the availability and continuity of IT resources in the event of a disaster. Service Level Agreements, between users and IT, can determine the level of support required to resume critical business operations. A disaster can be defined as an event that will exceed available IT services to the point of severely affecting business operations. Disasters can mean different things to different organizations: lack of email capability for a day may be trivial to some, but mission critical to others.

Effective contingency planning consists of a series of activities, all of which must change to reflect different the business processes. The activities are:

- Assessing potential risks
- Determining how to handle the risks
- Developing plans to deal with the risks
- Periodically test the plan
- Periodically update the plan
- Maintaining staff knowledge about when and how to implement the plan
- Implement the plans in the event a disaster occurs

Disaster Recovery is a structured approach to allow resumption of business activities when large-scale problems occur. These problems are normally caused by forces outside of the control of information technology, usually on the scale of floods, fire, etc. The procedure(s) for recovery must address 'above the data' issues, such as: the hardware and software platforms required to restart the applications, the steps to put all data/programs in place, and how to reconnect the end users to the application. Activities include:

- Off-site storage
- Planning, policies and procedures for data recovery
- Routine testing
- Data archival
- Library management
- File system management
- Tape and media management

The following levels of availability management should be considered when creating contingency plans (Kansas):

Business Support	Strategic Planning, Architecture Definition, Requirements Management, Planning & Control
Management Practices	Service, Change, Situation, Configuration and Project Management, Testing, Training, Acceptance, Human Resources
Applications	SDLC, Third Party Software, Data, Standards
Support System	Automation, Security, Middleware, Tools, Database, Output Management
Systems Software	Operating Systems, Protocols
Hardware	Processor, Storage, Communications
Facility	Construction, Environmental, Electro-Mechanical, Utilities

Principles

- ❑ Every agency will have contingency planning/disaster recovery process that includes periodic reviews and updates to protect critical data and applications.
- ❑ Service Level Management - Development and management of agreed to performance criteria and levels in support of business objectives.
- ❑ Test Management - Ensure that new or changed systems and applications work properly in an operating environment before production deployment.
- ❑ Configuration Management
- ❑ Change Management - Facilitate the introduction of change while reducing the risk and impact of changes to users.
- ❑ Recovery Management - Proactively plan and prepare for the actions necessary to execute a smooth and timely restoration of services following a disruption.
- ❑ Outage & Crisis Management - Managing a failure situation until service as been restored.
- ❑ Problem Management - Identify and resolve all problems impacting service. Provide feedback to user and take preventative action.
- ❑ Help Desk - Provide primary interface between users and IT for problem identification, problem resolution, and closed loop feedback.

Standards

Technologies

Change Management Domain

Description

The Change Management Domain defines the roles, policies, standards, and technologies for version control of all IT assets.

One meaning of managing change refers to the making of changes in a planned and managed or systematic fashion. The aim is to more effectively implement new methods and systems in an ongoing organization. The changes to be managed lie within and are controlled by the organization. However, these internal changes might have been triggered by events originating outside the organization, in what is usually termed “the environment.” Hence, the second meaning of managing change, namely, the response to changes over which the organization exercises little or no control (e.g., legislation, social and political upheaval, the actions of competitors, shifting economic tides and currents, and so on). Researchers and practitioners alike typically distinguish between a knee-jerk or reactive response and an anticipative or proactive response.

Strict change control procedures ensure that applications, systems, environments and networks been thoroughly tested and meet the standards set forth in this domain prior to release into production. Change Management allows co-ordination and control of updates to applications, systems, environments, and networks. This provides a means of making sure that changes have minimal impact when possible, or if not possible, that the impact is scheduled, fully understood, and proper support during the scheduled installation can be provided to minimize the impact to the users.

Purpose

A systems life cycle methodology refers to the process in place for requirements definition, system design, development, testing, delivery, support, ongoing change management, retirement of systems, and technology infrastructure. In other words, a framework governs a system from its conception to its final disposition. The change management portion is an important piece and as technology continues to expand at an incredible rate the need for change management increases as well.

Change management disciplines provide documentation of program and platform changes as systems evolve. These disciplines reduce the time for maintenance and the time for problem escalation. Also, change management saves the cost of reinstalling COTS software when new releases are available. Finally, change management protects the investment in software licenses by allowing for rapid upgrades required to maintain vendor support.

Service level Agreements are an effective tool ensuring that proper procedures for change management are followed, properly documented and executed in a timely fashion. Effective Service Level Agreements are the result of good working relationships and communication between the IT department and the users. Factors that affect service level management are:

- Business objectives
- Project budgets
- Organizational complexity
- Infrastructure planning

Because change management is a normal activity within the systems life cycle, the Change Management domain is closely related to the Applications Development domain. There is also a close relationship between the Help Desk/Problem Management domain and Change Management as the change is often initiated as a resolution to a problem or the identification of new requirement through the Help Desk.

Principles

Standards

Technologies

Category	Emerging Standard	Current Standard	Twilight Standard
Problem Mgmt.		Peregrine's ServiceCenter	Heat Support Magic Homegrown tools
Help Desk	GWI's Help! for Lotus Notes	Peregrine's ServiceCenter	Heat Support Magic Homegrown tools
Change Mgmt.	Peregrine's ServiceCenter		Manual processes
Configuration Mgmt	Peregrine's ServiceCenter		
Software Mgmt.	Peregrine's ServiceCenter	S/w distribution to desktops and LAN servers via: SMS ManageWise WRQ Express Z.E.N. Works Unicenter Veritas DMS Some use of apps from LAN servers. SoftTrack on some LAN servers	Managewise

Console/Event Management Domain

Description

The Console/Event Management domain defines the roles, standards, policies, and technologies for monitoring and controlling components of all collective hardware and software within the entity's data center, including large and mid-range systems.

Event management is a backbone of every enterprise management system, since it is the flow of events that describes various activities in the enterprise. By coordinating or acting on those events, enterprise starts being managed.

Console/Event Management allows you to monitor specific event conditions, such as loss of service or lack of storage, that occur in your network environment. Based on predefined events on nodes, databases, or listeners, the threshold parameters are set for which notification will be sent. Specific system administrators can be notified when an event condition occurs. For some events, the choice to execute a *fixit* job that automatically corrects the problem can also be set.

Purpose

The purpose of this domain is to establish guidelines and procedures that will ensure quick response to systems, applications, and network problems, to minimize human intervention, and maximize systems and network availability. Console/Event Management provides consistency and uniformity in monitoring activity from a central location and overall improves the quality of service through enhanced problem recording and reporting.

Console and Event management must be compatible and supportive of Networking hardware and networking management software, Platform and Storage Domains as well as the Business Continuity Domain, which covers contingency planning and disaster recovery.

Event management must be closely aligned with the Problem, Help, Change, and Asset Management processes due to their highly integrated natures.

Principles

- ❑ Event filtration should be enabled to eliminate alarms from non-critical and irrelevant devices.
- ❑ Every device should have a management element capability.
- ❑ System administrators at the agency level should have access to their data on the central management consoles.
- ❑ Events should be correlated and escalated based on the location and relevance of the system.
- ❑ System management must focus on increasing system stability and availability while reducing costs
- ❑ Systems management must facilitate business processes.
- ❑ The information gathered about events must be reportable and able to be quantified.
- ❑ The State should have the flexibility to dynamically change the criticality of any given device.

Standards

Technologies

Category	Emerging Standard	Current Standard	Twilight Standard
System Mgmt		SNMP Traps MS SMS Novell ManageWise Unicenter TNG	
Network Mgmt		SNMP Traps	
Application Mgmt		AMS ARM	
Agents, Protocols		SNMP V2 DMI Spec 2.0 Zero Admin Spec	CMIP
Console Mgmt	Unicenter		
Remote Operations		SMS ManageWise Unicenter	
Server Mgmt		SMS ManageWise Unicenter	
Workstation Mgmt		SMS ManageWise Unicenter	
Management Agent		SNMP MIB-2	

Data Management Domain

Description

The Data Management Domain defines the roles, policies, standards, and technologies for data definition, design, management, and administration as a recognized enterprise-wide resource. The Database domain provides a process-independent view of all enterprise-wide data stored and housed in a manner that enables Information Management while adhering to all Security and Privacy domain requirements.

The Data Management Domain is also tied closely to Information Management, Applications Development Management, and Data Storage Domains.

Should the connection to e-Commerce be mentioned here or would it be better to address Data Management as an important consideration within the e-Commerce Domain?

The Data Management domain includes non-embedded relational data management systems

Some examples include but are not limited to:

Access Standards
Product Standards
Data Warehouse
Data Stores
Data Definition Standards - Metadata (encyclopedia)

Extract, transform, load

Purpose

Historically data has been stored in multiple formats and multiple times throughout an enterprise, creating inconsistencies and difficulties in managing and retrieving information. Data is elemental in nature. It is the building block for all information and knowledge within an enterprise. New technologies such as Storage Area Networks and Knowledge Management software provide exciting opportunities for data storage and viewing.

A common architecture would eliminate a great deal of redundancy and inconsistent in information stored and updated in multiple locations. If data is stored and managed appropriately, it will yield valuable predetermined and indeterminate information. Citizens and state employees with access to information and knowledge bases will make better decisions and be able to make them in a timelier manner.

Data Management encompasses planning and overseeing the acquisition, relationships, organization, modification, distribution, usage, and retirement of data to support many uses. It involves obtaining enterprise-wide agreements about the definitions, attributes, and relationships of data, and directing and monitoring activities related to data standards, data dictionaries and repositories, documentation standards, data models, data base content management, and supporting data management applications. The affect of inadequate data management techniques has been dramatically illustrated through data warehouse efforts where up to 75% of total project costs are consumed in data “cleansing”.

Effective Data Management ensures accessibility between applications by all users (Agencies, Department, State/Local Governments, citizens/customers, trade associations, advocacy groups, and others), provides for and encourages reuse of data, ensures consistency of data, increased responsiveness to legislative programs and reduced application backlog.

- ❑ Databases should have a high degree of physical partitioning.
- ❑ Logical boundaries must be established between the partitions, applications or database and the logical boundaries must not be violated.
- ❑ Transaction processing (OLTP) should be separated from data warehousing and other end-user computing.

Principles

- ❑ Government data is an enterprise-wide resource. All primary data should be captured once at the point of creation, and stored and managed to enable appropriate levels of sharing across the enterprise, subject to Privacy requirements.
- ❑ We will aggressively promote the use of electronic data capture and discourage the use of paper forms for source documents. We will encourage the use of electronic service delivery and moving source data capture to the data source (e.g. via the Internet).
- ❑ Within policy, privacy, cost and performance constraints, we will make the most timely, accurate and complete data possible to our stakeholders.
- ❑ Data management procedures should insure that enterprise data is maintained in a manner that provides high availability, performance, and reliability to the end user.
- ❑ The data management architecture must be tested and conform to generally accepted industry standards.
- ❑ Data management architecture should be based on commonly accepted extensible, interoperable, and scalable industry standards.
- ❑ Data management procedures must address and insure confidentiality of records that contain information that is limited for open/public access.
- ❑ In all cases, agencies should carry out data management activities utilizing proven and stable IT products and processes.

Standards

- NIST FIPS PUB 156 (IRDS) Data dictionary/directory services
- NIST FIPS PUB 127-2 (SQL) Data base language SQL
- NIST FIPS PUB 193 (SQL Environments) Data management system

Technologies

Organizations are moving towards the total digitization of all forms of corporate data and the creation of enterprise-wide data warehouses.

- Multimedia data types, not just text
- Data Warehousing
- Data persistence, cross-stovepipe
- Knowledge Management
- Search & retrieval, workflow, data visualization
- Impact on tools, business processes, security

Industry Trend - Intelligence"-oriented technologies are becoming increasingly available from commercial vendors.

- DW, KM, GIS, Imagery, Analysis Tools, Language Translation, Agents, targeted news services, etc.
- Explosion in commercial information security tools and methods
- Impact on Buy vs. Build decision

Products
- DB2
- ORACLE
- SQL

Standards
- ODBC
- Protocols

Data Storage Domain

Description

The Storage domain defines the roles, policies, standards, and decision-making criteria for the acquisition and deployment of data storage media, as well as the policies governing archiving of data and the use of storage facilities.

Because of the increasing requirements for data not only within departments, but also across agencies, from the citizens and public and private providers, it is critical that data be available on a continual basis. Availability of data has become a mission critical part of government business. With the variety and complexity of systems and applications today, unplanned outages are inevitable. In such cases, it is imperative that backup data be stored on the media appropriate to its criticality and need.

Data considerations from the Data Management domain must be considered when implementing policies and procedures for this domain. Security issues are not covered under this domain, therefore, but rather within the Security domain. Because of the relationship between Data Storage and data recovery this domain is also tightly linked to the Business Continuity domain.

Purpose

The purpose of this domain is to determine the types of media and storage facilities required based on the criticality of the data and the frequency of use. The means of storage and locations, as well as standards governing backup procedures, retention and recovery procedures are required and should be fully documented.

Storage should be fault-tolerant based on the criticality of the data and application access to the data. Fault tolerant storage is a costly venture and it is important to determine the appropriate use to this means of storage.

Because there is and will be a need for increased storage as the sharing of data continues to increase, the scalability of storage solutions should be an important consideration.

Best Practices & Processes

- Move infrequently accessed data to cheaper media.
- Move frequently accessed data to faster media.
- Storage should be a centralized as applicable.
- Raid levels should be used as follows:
    - 0 (disk striping) offers high performance for full-motion digital video, and database applications by reading and writing data across several drives at one time.
    - 1 (disk mirroring) provides full data redundancy for system and other critical disks. Every write operation is duplicated on up to four separate drives - providing an on-line, real-time backup of valuable data.
    - 5 (parity and data striped) works well in read intensive environments. Although write caching often offsets the poor write performance associated with this level. Since parity information is used, a RAID 5 stripe can withstand a single disk failure without losing data or access to data.
- Storage solutions should be designed with scalability.

- Storage should be flexible, re-configurable, and tolerant to change to provide low total cost of ownership.
- High availability data protection strategies (mirroring, replication, etc.) should be employed for disaster tolerance.

Principles

❑ Data management and protection at all levels is consistent

❑ Backup, recovery and Disaster Recovery of all critical data is essential

Standards

Technologies

eCommerce Domain

Description

The E-Commerce Architecture defines the standards, technologies and guidelines for electronic commerce among state agencies and between state agencies/entities and outside entities. The eCommerce Architecture also defines how the government conducts electronic business with the citizens.

The next generation eCommerce must be founded on open standards, an extensible architecture, and distributed, object-oriented components that deliver to businesses the tools necessary to build custom, dynamic business logic for the Internet.

Purpose

Principles

Standards

Technologies

Electronic Collaboration Domain

Description

The Electronic Collaboration domain defines the standards and infrastructure components that facilitate the interaction of the workforce and promote group productivity. These include e-mail, directory services, and other person-to-person or group collaboration tools.

The market-driven complexity and integration capability of Workgroup Services products will create increasing demands on system resources: processing power (speed and memory), operating system features, and network bandwidth. Network-centric/thin client designs, the option which requires the least impact on user desktop machines, is critically dependent on high-speed, highly reliable, very secure network connections. Changing from a paper-based organization to a "digitally-based" organization will require significant investment in infrastructure capacity, reliability and security. Within Kansas state government, the necessary investment in Workgroup Services will receive requisite support only when it is clearly cost-justified in terms of service to the citizens of the state

Purpose

The Electronic Collaboration domain describes Workgroup Services: practices, typically software related, that allow for data to easily be shared between different agencies, bureaus, and departments. Other domains such as Application Development and Management and Asset Management describe the process of developing and tracking COTS software licenses, etc.

Office automation software provides administrative support for completing daily business functions. This element is defined as including, but not limited to, the following:

Spreadsheets
Business Graphics
Presentation Packages
Personal Data Bases
Word Processing
Project Management and Scheduling
Calendars
Desktop Publishing
Multi-media
Terminal Emulation
Web Browser
Document Imaging
Mail
Groupware
Executive Information System (EIS)

The applications listed are built utilizing the services defined by the open system architecture.

Office automation is an inherent aspect of the office environment and is key to enabling employees to carry out the day-to-day business of the agency. Increasingly, the use of office automation will support the need of the public to receive information in electronic format.

Principles

- E-mail service should be available at all times from any location. Time, distance, and location should not restrict e-mail service.
- Workgroup services require a consistent infrastructure and communications backbone to support collaboration and communication. Reliable network performance is absolutely critical to the conduct of business when business operations depend on electronic workgroup services.
- Content exchange, directory services, and authentication services are key infrastructure components necessary to facilitate communication and collaboration.
- The system supporting electronic workgroup services must have built-in recovery capability, such as redundant servers and data storage devices.
- Workgroup services will enable the capability to work at any time from any place.
- Information related to a single event, in whatever form, media or storage location, should be maintained and made accessible as a record unit.
- When state organizations plan adoption of new technology to provide integrated information services, they should consider functionality (proven through demonstration), likelihood of long-term viability (as reflected in market acceptance), and the probable cost to integrate or migrate to the new technology.
- Workflow systems should subscribe to the standard interface with other workflow systems for the purpose of passing and processing work items between business units and processes.

Standards

- ITU-T X.400 Mail and X.500
- Internet RFC 821 SMTP
- Internet RFC 1327/1495 (SMTP to X.400 gateway) Application-oriented network services
- Internet RFC 1041 (TN3270) Access to mainframe systems
- Internet RFC 1647 (TN3270E) Access to mainframe systems
- NIST FIPS PUB 1-2 (Code for Information Interchange) Characters and symbols – Character sets
- ISO 11172-1,2,3:1993 (MPEG) Compression - Motion image compression
- ISO/IEC 10918-1 (JPEG) Compression – Motion image compression
- X/Open C436:1994 (Commands and Utilities) Compression - Text and data compression
- NIST FIPS PUB 152 (SGML) Document interchange – Custom definition of document types
- NIST FIPS PUB 152 (SGML) Document interchange – Document exchange
- NIST FIPS PUB 177 (IGES) Technical data interchange – Vector graphics data interchange
- ISO/IEC 9592-4:1992 (PHIGS PLUS) Vector graphics – Vector graphics API
- NIST FIPS PUB 153 (PHIGS) Vector graphics -Vector graphics API
- NIST FIPS PUB 128-1 (CGM) Vector graphics -Vector graphics data interchange
- HTML (HyperText Markup Languages) 3.0
- HTTP (NCSA Standard NTTP protocols)

Technologies

Collaborative computing environments are enabling organizations to better marshal and focus their intellectual resources.

- Explosion in multimedia collaboration tools
- Collaboration as new & improved way to do business
- Distributed, ad-hoc & transient communities of interest
- Collaboration both inside and outside of organizations

Architecture Component	Emerging Standard	Current Standard	Twilight Standard
E-mail		• SMTP • MIME • IMAP4 • POP3	• OV/VM • IMAP3 • POP2
Document Format	• XML	• .rtf • .txt • .pdf	
Spreadsheet			• SYLK
Images	• JPEG 2000 • SVG	• .bmp • TIFF • GIF • JPEG • MPEG	• Proprietary
Document Digitizing		• TWAIN • ISIS	
Character Recognition			
Document Endorsement and Authentication	• Digitized signature • Digitized signature with biometric data • PKI digital signature (X.509v3) • Biometric imprint	• Physical signature	
Directory Services	• LDAP • Active Directory • DSML	• NDS • X.500	
Calendaring	• ICAP • iCalendar		
Records Management		• DOD 5015.2	
Financial Reporting	• XFRML		
Enterprise Report Management		• APF • Metacode	
Document Management	• DMA • ODMA		
Workflow	• WFMC		
Workgroup Collaboration			
Videoconferencing			
Telephony, IVR, Voice Mail			
Voice Recognition			
Electronic Forms	• XHTML Extended Forms • XFA	• XFDL	• OFDL • OFML
File Viewer			
Multimedia	• MP3		
Business Graphics			
Engineering Graphics			
Geographic Information Systems (GIS)			
Web Publishing	• XML	• HTML • SGML	

GIS Domain

Description

GIS is a computer system capable of assembling, storing, manipulating, and displaying geographically referenced information, i.e. data identified according to their locations. GIS involves computer-based tools for mapping and analyzing data that integrate common database operations such as query and statistical analysis with the visualization and geographic analysis benefits offered by maps. GIS is a multi-faceted system of hardware, software, data, people, and methods. GIS technology has many capabilities and benefits, making it possible to perform complex analyses, resource management, and development planning.

The GIS Architecture defines the standards and technologies for implementation of Geographic Information Systems

Purpose

GIS provides facilities for data capture, data management, data manipulation and analysis, and the presentation of results in both graphic and report form, with a particular emphasis upon preserving and utilizing inherent characteristics of spatial data. GIS and related technology will help in the management and analysis of large volumes of data, allowing for better understanding of terrestrial processes and better management of human activities to maintain world economic vitality and environmental quality. Agencies will use GIS technology for a multitude of functions. The results will provide high quality customer service and reduce cost and increase partnerships between federal agencies, state and local organizations.

Principles

A formalized user need analysis is absolutely critical to the successful implementation of GIS technology.

Development of the benchmark should include a consideration of other roles within the organization that may require integration with the GIS technology.

Due mostly to this diverse range of different architectures and the complex nature of spatial analysis, no standard evaluation technique or method has been established to date.

Any GIS should be evaluated strictly in terms of the potential user's needs and requirements in consideration of their work procedures, production requirements, and organizational context!

The acquisition of GIS technology should not be done without seriously considering the way in which GIS will interact with the rest of the organization.

A successful GIS operates according to a well-designed implementation plan and business rules, which are the models and operating practices unique to each organization.

Standards

The Federal Geographic Data Committee (FGDC), supports the development of the National Spatial Data Infrastructure (NSDI). The FGDC has developed, and/or is developing, numerous thematic geo-spatial data standards to guide the development of the NSDI.

SDTS - http://mcmcweb.er.usgs.gov/sdts/whatsdts.html

The Spatial Data Transfer Standard, or SDTS, is a robust way of transferring earth-referenced spatial data between dissimilar computer systems with the potential for no information loss. It is a transfer standard that embraces the philosophy of self-contained transfers, i.e. spatial data, attribute, geo-referencing, data quality report, data dictionary, and other supporting metadata all included in the transfer.

Purpose of SDTS

The purpose of the SDTS is to promote and facilitate the transfer of digital spatial data between dissimilar computer systems, while preserving information meaning and minimizing the need for information external to the transfer. Implementation of SDTS is of significant interest to users and producers of digital spatial data because of the potential for increased access to and sharing of spatial data, the reduction of information loss in data exchange, the elimination of the duplication of data acquisition, and the increase in the quality and integrity of spatial data. SDTS is neutral, modular, growth-oriented, extensible, and flexible--all characteristics of an "open systems" standard.

The SDTS provides a solution to the problem of spatial data transfer from the conceptual level to the details of physical file encoding. Transfer of spatial data involves modeling spatial data concepts, data structures, and logical and physical file structures. To be useful, the data to be transferred must also be meaningful in terms of data content and data quality. SDTS addresses all of these aspects for both vector and raster data structures.

SDTS was approved as Federal Information Processing Standard (FIPS) Publication 173 in 1992 after 12 years of development and testing and in 1994 became mandatory for federal agencies. SDTS is available for use also by state and local governments, the private sector and research and academic organizations. From: "Dan Henke" dhenke@mercury.er.usgs.gov

Other standards that pertain to GIS include:

- The Open Geodata Interoperability Specification (OGIS), is "a comprehensive specification of a software framework for distributed access to geodata and geoprocessing resources. OGIS will give software developers around the world a detailed common interface template for writing software that will interoperate with other OGIS compliant software written by other software developers". (USDA)
- Vector Product Format (VPF) is a military standard for vector-based digital map products produced by the U.S. Department of Defense (DOD).
- ANSI
- ISO

Technologies

Categories	Emerging	Current	Twilight
• Geo-spatial (GIS) Metadata		• ITEC Policy 5100, Kansas GIS Metadata Std (FGDC-STD-001-1998 V2.0, CSDGSM)	

Categories	Emerging	Current	Twilight
• Geo-spatial (GIS) Thematic Data	• FGDC Classification of Wetlands and Deep Water Habitats • FGDC Vegetation Classification Std • FGDC Soils Geographic Data Std • FGDC Std for Remote Sensing Swath Data • FGDC Content Standard for Digital Geo-spatial Metadata, Part1: Biological Data Profile • FGDC Utilities Geo-spatial Data Content Std • FGDC Spatial Data Content Std, Computer-Aided Design and Drafting Profile • FGDC Geo-spatial Positioning Accuracy Std, Part 4: Architecture, Engineering, Construction, and Facilities Management • FGDC Content Std for Framework Land Elevation Data	• Kansas Geodata Compatibility Guidelines V. 2.2 • Kansas GIS Cadastral Std • Kansas GIS Addressing Std • Kansas GIS Hydrography Std • Kansas GIS Administrative Boundaries Std • FGDC Geo-spatial Positioning Accuracy Std, Part 1: Reporting Methodology • FGDC Geo-spatial Positioning Accuracy Std, Part 2: Standards for Geodetic Networks • FGDC Geo-spatial Positioning Accuracy Std, Part 3, National Std for Spatial Data Accuracy • FGDC Content Std for Digital Orthoimagery • FGDC Spatial Data Transfer Std • FGDC Spatial Data Transfer Std, Part 5, Raster Profile • FGDC Spatial Data Transfer Std, Part 6, Point Profile	

Help Desk/Problem Management Domain

Description

The Help Desk/Problem Management domain defines the roles, standards, policies, and technologies for monitoring and controlling problem reporting and resolution. By its very nature this domain relates closely to Asset Management, Console/Event Management, Change Management and Business Continuity. Security and Privacy are also major considerations of the Help Desk/Problem Management domain.

Purpose

In years past the Help Desk focus was aimed primarily upon requests and or problems pertaining to mainframe systems or desktop services. In recent years, with the expansion to more distributed systems, as well as the introduction of the Internet and web-enabled applications the diversity of knowledge required by help desk staff has raised exponentially. Help desks are now called upon to support a broad range of applications on varying platforms, and with diverse levels of complexity. Often the problems needing resolution lie ultimately with vendors and may also cross agency lines, state lines, or even cross country, and beyond.

Along with the increased demand for diverse support, the timing for response has also become a critical factor. It has therefore become essential to incorporate service level agreements and have dynamic help desk/problem management tracking and escalation applications. The help desk personnel are the central means for change management notifications as well as event management.

Systems have become more complex, employees as well as citizens are using the computers for more and varied purposes, and often these are people with little or no prior experience with computer systems. They can become easily frustrated and often the help desk is the one place where citizens and employees can get assistance from another human. Is it important that users know where to call for assistance and the help desk have the information they need to assist users in all situations. Wherever possible, the problem tracking and error notifications should be automated and warnings/notifications of scheduled or non-scheduled downtimes should be automated and available for quick reference.

The staff need to be cognizant of Privacy data and are an excellent source for promoting the importance of security for the systems they support.

The following goals are important to this domain:

- Maximize end user satisfaction.
- Improve communications with customers.
- Have in place well-defined and documented procedures for problem reporting and resolution.
- Majority of problem/help calls resolved at first contact.
- Rapid escalation to knowledgeable resources.
- Improve time to resolution.
- Tracking and follow-up procedures to ensure timely resolution and customer notification.
- Be able to identify educational needs within the user community.
- Foster customer self-sufficiency.

Principles

- There should be a common data architecture for problem identification.
- Each agency will have access to a common call management and help system tool for problem reporting and help desk activities.
- The problem management database should conform to standard access methods to facilitate reporting and data analysis requirements.
- Help desk personnel should possess superior communication skills and be thoroughly knowledgeable of supported products and facilities.
- Help desk personnel should be as knowledgeable of the organization's business practices as possible.

Important factors: (KS)

- Document things the first time; provide handouts of processes and procedures to users. Set up a help desk FAQ web site and or Email address.
- Have a central help desk to record and process all requests for support.
- The Problem Management initiatives/solutions must include representatives from the complete customer base, additional activities should not proceed until documented and approved customer requirements have been developed.
- Existing information should be used through the interim process flow: Severity Codes and Processes, Escalation Information, and Notification Matrices. These flows are staged through the N tiers of support with the goal of resolution of 80% of the requests through the first tier in 15 minutes or less.
- Rigorous review and approval cycles should be implemented to define Metrics and Measurements, Problem Screens and Schemas, Performance Requirements, and Change Component/Asset information.
- Specific measurement and metric report information must be specified in order to prevent after the fact efforts that may or may not gather the correct information, or the correct intervals, associated with the correct support groups.
- Any problem management database should conform to standard access methods to facilitate reporting and data analysis requirements.
- Simulate actual operating conditions to identify procedures, processes, personnel, and tool deficiencies, (manage your expectations).
- Identify a plan that anticipates challenges associated with achieving desired business goals, (80% first call resolution), and work closely with Help Desk Management to address and preferably resolve these "early" in the year.
- Perform periodic audits and surveys of customers, help desks, Tier 2/3 personnel, and application support personnel to verify that current Problem Management functions and capabilities still meet operation requirements. Plan and implement changes accordingly.
- Automate as many of the current interim manual processes, (Severity 1 and 2 communications).

Standards

Technologies

Any problem management database must be ODBC and SQL compliant.

Information Management Domain

Description

The Information Management Architecture describes the logical structure of databases and the methodology used to correlate data in multiple databases. Information management focuses on tools and business processes required for establishing and maintaining an enterprise-wide approach to the use of corporate data. The information architecture provides a framework for defining responsibility for data integrity and distribution. The information architecture ensures that all government entities as well as the public will have efficient, effective, and convenient access to accurate and current government information, as appropriate, under laws and policies governing security, privacy, and freedom of information.

Data and the exchange of data within the enterprise is the key to all aspects of government and is therefore it's primary asset. Because of this the information must be protected from loss or corruption in any form. In order to protect the rights of the citizens, privacy standards and regulations must be strictly enforced. Therefore, this domain is closely linked with the Privacy and Security domains.

This domain also ties in closely to the Data Management, Internet/Intranet and Accessibility Domains because of the need to coordinate on the definitions for the purpose of providing information for analysis and ensuring that the information is appropriate, accessible and beneficial across agencies as well as to the public.

Purpose

The purpose of the Information Management Domain is to maximize the usefulness of recorded information by assuring that it is usable for multiple purposes and can be found quickly and easily; and maximize the business contributions from the personal knowledge and intellectual skills of employees, encouraging the development of technologies to support the flow of data within agencies, as well as across agency lines.

The goal is to build data quality into new systems as well as incorporating it into existing systems. This includes the establishment of procedures and processes to avoid the redundant efforts to collect, maintain and store data, and provide methods for sharing transaction data as well as summary data, meta data, historical and external data. The use of common techniques and open standards will promote interoperability among systems and will identify opportunities for sharing commonly used data through integrated applications and databases.

Should Transaction processing be discussed within this domain?? If so, see Transaction Processing under Data Mgt Domain file for applicable standards, etc.

Principles

- Continually seek to improve the quality, accuracy, and integrity of enterprise information through the promotion of data consistency and standardization.
- Continually strive to improve data management and access through the use of appropriate existing and new methods, tools and technologies.
- The business functions and initiatives shall shape and drive the conceptual, logical and physical models of data and information assets.

- Entities must facilitate data and information sharing within the organization and with external user groups.
- Data and information resources are assets that must be managed as valuable resources, held in trust for the public.
- Data and information management practices and policies pertain to the entire lifecycle of the asset including its
  a. Creation
  b. Use
  c. Storage
  d. Documentation (metadata)
  e. Disposition or archival.

Standards

The need for these standards will become increasingly more important as more mission critical inter-agency data and workflow sharing systems are deployed. Currently there are two converging standards for metadata, the first from the Meta Data Coalition (MDC) and the second from the Object Management Group. The two groups are working together on developing a Unified Modeling Language (UML). UML is a language for specifying, constructing, visualizing, and documenting the artifacts of a software-intensive system.

- MDC Open Information Model 2.5, 2.6, 2.7 at: http://www.mdcinfo.com/OIM/MDCOIM11.html
- Object Management Group standards: CORBA, UML, and Workflow at http://www.omg.org
- Workflow Management Coalition Standards (WfMC). http://www.aiim.org/wfmc/standards/docs/tc1023v10beta.pdf

Technologies

Categories	Emerging	Current	Twilight
• Metadata • Analysis and design • Database and warehousing • Object and component design • Knowledge management • Business engineering	The Open Information Model Meta Data specification: • UML as a base model. • XML for metadata interchange. • SQL for data retrieval. (Refer to Meta Data Coalition at http://www.mdcinfo.com/)		

Internet/Intranet Domain

Description

The Internet/Intranet Domain defines the roles, policies, standards, and technologies that provide the framework for the electronic delivery of information and services to every government agency, business or citizen as deemed permissible under privacy and other mandated regulations.

Purpose

The Internet and the focus on electronic government provide unprecedented opportunities for improving the way we do business. In the next 5 years, an estimated 80% of applications will be based on or extended by Internet derived technologies.

The Government Paperwork Elimination Act (GPEA), Title XVII of Pub. L. 105-277, provides for Federal agencies, by October 2003, to give persons who are required to maintain, submit, or disclose information the option of doing so electronically when practicable as a substitute for paper, and to use electronic authentication (electronic signature) methods to verify the identity of the sender and the integrity of electronic content. The Act specifically provides that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

This will open up the use of the Internet as the means for "virtual" government.

If government is to continually improve the quality and accessibility of the services, its laws mandate, and its constituent's desire, it is critical that a coherent, consumer driven Internet presence be established and maintained. Consumers have the right to expect that government agencies provide appropriate electronic access to information and services and that they act as responsible stewards of the financial resources provided it to accomplish this mission.

The extension of access to data and services through intranets, extranets and the Internet is a cost effective strategy that leverages the investment in information technology. Virtual access increases the efficiency of service delivery systems and reduces costs by eliminating redundant delivery systems and costs associated with time lags and delays. (Kansas)

Principles

- ❑ Internet design, development, delivery and management should focus on the needs and capabilities of the government customer

- ❑ Graphic design, information design, and interaction design should conform user-centered design concepts of the enterprise site, to maximize the ease of use for the citizen.

- ❑ An open architecture will assure ease of use, accessibility, reliability, scalability, and a targeted customer focus.

- ❑ Internet standards should be flexible and extensible to allow for responsive use of technology and business practice improvements.

- ❑ Internet standards, practices and methods should address the issues of data management, record retention, information and transaction confidentiality, and security.

- ❑ Access to government information and services should be based on customer needs and not on the government organizational structure.

- ❑ Agencies should use common principles of usability testing to assess the effectiveness of actual and proposed information and service delivery, and incorporate the results of such testing into both the graphic and interaction design processes.

- ❑ Agencies will develop and implement solutions according to defined technology standards. Statewide and industry standards will be adopted.

- ❑ The State, departments and agencies will actively seek opportunities to reduce costs by enabling sharing and/or re-use of I/T assets with, as appropriate, other states, departments, and agencies. I/T assets include data, hardware, software, networks, applications, application components, knowledge and skills.

- ❑ A standard set of proven technologies should be used: the proliferation of technologies will be avoided.

Standards

Technologies

Category	Emerging	Current Standard	Twilight Standard
Encryption		SSL3 and SSL2	
Transmission Protocol		IP/UDP	IPX
Messaging Protocol	IMAP4	SMTP MIME-compliant LDAP	
Mgmt Protocol	SNMP V2.0	SNMP V1.x	CMIP
Domain Naming		DNS	
Object Architecture	COM+ IIOP	CORBA 2.0 OLE/DCOM	
RDBMS Access	JDBC	ODBC	
RDBMS Language	SQL93	SQL92	
Transaction Management		X/Open X/ATMI	
Transactions		X/Open TX	

Industry Trend

The Internet will drive the technical standards for network computing.

- Web & Internet based technology used everywhere
  - Network computing model
  - Transparency of Internet/Intranet technology
    - Inside and outside of organizations
- Impact on clients, servers, network & application (business) logic
- Browser as predominant user interface for network applications
- Impact on next-generation telephony

Middleware Domain

Description

User Interface domain defines the components that create an integration environment between the user workstations and legacy and server environments to improve the overall usability of the distributed infrastructure. Middleware provides interfaces between applications and network communications mechanisms. Middleware functions to create uniform mechanisms for application integration independent of network and platform technologies.

Examples of middleware include applications servers, transaction-processing monitors, message-oriented middleware, object request brokers, object transaction monitors, remote procedure call services, integration brokers (including message brokers), business process managers (including workflow services), and database gateways.

Purpose

The User Interface domain includes technologies to integrate systems. It functions to create uniform mechanisms for application integration independent of the network and platform domains. While the components do provide interface between components within the Knowledge Management, Application Engineering, and Database domains, it does not include those components.

User Interface domain provides a standardized approach that allows for the preservation of legacy systems and information resources while facilitating the incorporation of new capabilities and emerging technologies. The continued emergence of new capabilities and information resource technologies dictates a comprehensive approach that provides the state an environment that can adapt to these continual changes.

Standard guidelines provide significant cost savings through reuse of knowledge and applied architecture. This standardization also allows the state to implement a more financially tolerable approach to upgrading existing resources and implementing new systems and capabilities.

Some examples of middleware include, but are not limited to

CORBA
MQ Series
CICS

Principles

- ❑ Messaging is required to implement an adaptive systems architecture
- ❑ The interfaces across separate logical boundaries must be message-based.
- ❑ The message-based interfaces must extend to both customers and suppliers.
- ❑ Asynchronous communications should be used whenever possible to increase performance and scalability.
- ❑ Messaging should be employed as the communication between components in separate logical tiers.
- ❑ Isolating applications from data enables better flexibility to respond to changing business needs, new technologies and new design techniques.

Motivation

- Messaging technology is complex, but using messaging technology is easy to accomplish
- Messaging allows for location, DBMS, and data structure transparency
- Messaging is a key enabler for many of these best practices

Implications

- A messaging infrastructure is necessary
- Common messaging formats, ids and standards must be established
- Developers must learn how to use messaging
- Messaging does not require physical partitioning
- Network traffic may increase, unless asynchronous logic is used
- Applications must be designed to be event driven

Standards

NIST FIPS PUB 173-1 (Spatial Data Transfer Standard) Geospatial data exchange

NIST FIPS PUB 1-2 (Code for Information Interchange) Characters and symbols - Character sets

ISO 11172-1,2,3:1993 (MPEG) Compression - Motion image compression

ISO/IEC 10918-1 (JPEG) Compression – Motion image compression

X/Open C436:1994 (Commands and Utilities) Compression - Text and data compression

NIST FIPS PUB 152 (SGML) Document interchange – Custom definition of document types

NIST FIPS PUB 161 Electronic Data Interchange

NIST FIPS PUB 177 (IGES) Technical data interchange – Vector graphics data interchange

ISO/IEC 9592-4:1992 (PHIGS PLUS) Vector graphics – Vector graphics API

NIST FIPS PUB 153 (PHIGS) Vector graphics -Vector graphics API

NIST FIPS PUB 128-1 (CGM) Vector graphics -Vector graphics data interchange

Technologies

HTML/XML

Network Management Domain

Description

The Network Management domain defines the roles, policies, standards, and technologies that manage the communications infrastructure for the state's distributed computing environment. It defines the structure, topologies, bandwidth management, carrier services, and protocols necessary to facilitate the interconnection of the state's information resources, including those facilitating e-Government initiatives. Included in this domain is the definition of Intranet networks, Virtual Private Networks, and external connections to external networks including the Internet. This includes consideration for public access from private and Kiosk workstations, wireless drivers, and PCs.

Purpose

As industry develops new technologies and business and public demands access to more and more information, the complexity of Network domain increases. Standard Network Architecture guidance is required to ensure the access demands of the state and its citizenry are met in a cost effective manner.

Well-defined roles and standards provide clarity in purchasing and deployment objectives and contribute to strong compliance control points. Standards provide efficiency in costs, including purchase power, standardized training programs, and focused staff recruiting efforts. It lessens the complexity of systems management and administration. Overall it enhances the potential of meeting the increasing data access and system performance expectations of the state and its citizenry.

Principles

- ❑ The network must be manageable anywhere and at any time.
- ❑ Agency-based, non-central network management will be avoided whenever possible to reduce costs and provide consistency of service.
- ❑ Network management must be consistent with the Network Architecture.
- ❑ Network management must be consistent with the System Management Architecture..
- ❑ There should be no single point of failure, i.e. two network paths instead of one for major service domains
- ❑ Performance measurements should be adhered to, based on the acceptable levels determined and agreed to by the enterprise.
- ❑ WAN and most LANs should be managed centrally, some local control of agencies is acceptable behind their own router.
- ❑ There will be a consistent set of standards for network firewalls, virtual private networks, and general network security.

Standards

ISO
IEEE
ANSI

Technologies

Category	Emerging Standard	Current Standard	Twilight Standard
Network Monitoring		HP OpenView	Home-grown tools
Network Capacity		NG Sniffer Lanalyzer RMON Probes	
Router Management		CiscoWorks Cabletron's Spectrum	
NIC Cards	Remote Wake-up DMI PXE BootP NCP RIPL		
Management Protocol		SNMP 2.x MIB-2	CMIP Novell SNMP 1.x

Technology Trend - Enterprises are using new technologies to reduce administration costs and establish a unified system management approach for corporate computing.

- Return to Centrally Administered Computing
- NetPCs, WebPCs and Thin Clients
- Network and System Management Tools
- Server-centric Business Operations
- Enterprise desire to reassert centralized control of IT
- Mainframe mindset exploiting latest client/server technology

Physical Network Domain

Description

The Network domain includes network infrastructure for the computing environment. It provides reliable communication for the State's distributed information processing environment. The Physical Network domain consists of infrastructure elements, physical components (i.e. wiring, LANS, hubs), carrier services (i.e. frame relay, leased channels, ATM), and protocols (i.e. access routing and naming). It does not include user workstations, server platforms, or their operating systems.

Some examples types of networks include but are not limited to:

- WAN
- LAN
- Internet
- Intranet

Some examples of Physical Components include but are not limited to

- Wiring
- LANS
- Hubs
- Routers

Some examples of connects include but are not limited to

- Frame Relay
- ATM
- T1 Leased Lines

Some examples of Protocols include but are not limited to

- IP
- IPX
- SNA

Purpose

Networks are the essential enabling technology for client/server, Internet and collaborative computing. Lack of robust network architecture will impact the success of distributed applications. There is an increased need for access to information across the enterprise. Access must be seamless to reduce decision-making cycle times, therefore, states must implement an enterprise wide backbone network that provides a "single network image" as if it were a virtual, enterprise wide LAN.

The implications are the need for directory services, high speed, increased bandwidth, interconnection of distributed LANs, and legacy connection to client/server and Internet applications.

Uniform network architecture will enable LANs within the WAN to inter-operate while allowing a broad platform on which to run applications as needed. Such interoperability requires cooperation at all agency levels, and consistency in network components (e.g., wiring, hubs, servers, operating systems, and protocols), management practices, and services.

Principles

- Agencies will develop and implement solutions according to defined technology standards. Statewide and industry standards will be adopted.
- Standardization on layered protocols provides user transparency.
- The network architecture should be based on a set of standards that will enhance the availability of network support and provide a foundation upon which support planning can take place
- The network architecture should be based on a set of standards that will support the use of networks for integrated voice, video, image and data transmission
- The State, departments and agencies will actively seek opportunities to reduce costs by enabling sharing and/or re-use of I/T assets with, as appropriate, other states, departments, and agencies. I/T assets include data, hardware, software, networks, applications, application components, knowledge and skills.
- Agencies will use a standard set of proven technologies, such that the proliferation of technologies will be avoided to ensure stable long term viable technology and application environment.
- Future LANs must provide mechanisms for addressing quality of service.
- Telecommunications infrastructure planning is an integral part of facilities planning, leasing, maintenance, construction, and renovation

Standards

Technologies

Technology Trend - Networking performance and capacity is exploding.

- Performance/Bandwidth currently seen as shortfall, but…
- Now on verge of explosion with growth faster than Moore's Law
- Bandwidth becomes "free" in US and developed world
- Politics will still be cost factor in parts of world (tariffs, national PTTs, etc.)
- Domination of TCP/IP
- Domination of Ethernet

Category	Emerging Standard	Current Standard	Twilight Standard
Media	Category 6, 7 UTP	Category 3 UTP (voice only) Category 5 UTP Multimode fiber Singlemode fiber	Category 3 UTP (except voice) Coax Twinax
Topology		Star Mesh Point to Point	Bus Ring Multidrop
OSI Physical Layer	1000BaseT Ethernet	10BaseT Ethernet 100BaseT Ethernet Full Duplex Ethernet	10Base2 Ethernet Ethernet repeaters, hubs, concentrators
OSI Data Link Layer		Ethernet Ethernet Switching VLANs	Ethernet Bridges HDLC/SDLC Bisynch NetBEUI Netbios Token Ring
OSI Network Layer	Layer 3 Switching MPLS PIM SM IP V6	Internet Protocol (IP) V4 Asynchronous Transfer Mode (ATM) Routers	SNA X.25 IPX Appletalk DECnet
OSI Transport Layer		Transmission Control Protocol (TCP)	
Routing Protocols	MBGP	OSPF BGP4	RIP
Quality of Service	MPLS RSVP DiffServ	Over Provisioning Network Capacity TDM FDM Ethernet Packet Prioritization (802.3 P and Q)	
Carrier Services		Fractional T1 T1 T3/DS3 OC3-12 Frame Relay SONET ATM	9.6-56k
Wireless Transport	VSAT	Laser Infrared RF Cellular Microwave	
Wireless Protocol		Various, proprietary and defacto standards	
Network Security Services		VPN SSL IPSEC Ethernet Switching Encryption	Scrambling Ethernet Hubs

Category	Emerging Standard	Current Standard	Twilight Standard
Directory Services	LDAP	DNS registration X.500 NDS for Novell MS Domains	
Information Outlet	Fiber	RJ45 RJ11 (voice)	RJ11 (except voice)
Remote Access	XDSL	PPP V.90 ISDN BRI ISDN PRI Cable	SLIP Bell 212a V.32 V.32bis V.34 V.34bis
File Access and Transfer Services		TFTP FTP NDM	FTAM TSO Transmit IND$file NFS
Terminal Handling	Winframe for PC clients	TN3270 Telnet RAS 5350 X-windows	3270 Terminal Emulation
Remote Monitoring, Management		SNMP Version 1 and 2 Management Information Base (MIB) - IEEE RFC 1398 MIB II RMON 1 and 2 Out of Band Dialup Access	Proprietary

Voice Network

Category	Emerging Standard	Current Standard	Twilight Standard
Telephone Equipment	Voice over other technologies (IP, ATM, frame relay)	Analog Digital Proprietary	Key System
Trunking		T-1 Digital Transmission Link	analog trunks
PBX		enterprise, client-server based	non-enterprise PBX

Platform Domain

Description

The Platform defines the roles, policies, standards, and decision-making criteria for the acquisition and deployment of computing and data storage hardware and its operating software and systems. The Platform domain provides for the inclusion of industry standard platforms in use by users and the citizenry to enable e-government access. Components of the platform domain range from enterprise class servers to workstations and hand held computing devices and the operating systems (not applications) that run on these devices.

Purpose

The Platform domain addresses the acquisition and deployment of computing and data storage hardware and their operating software and systems. The domain has relationships but does not include communications infrastructure components, resident applications, or middleware. It also does not include the security and privacy aspects associated with deployment of these technologies. The Middleware Architecture, Network Architecture, Security Architecture, and Privacy domains need to be referenced for guidance on those aspects associated with implementation of these technologies.

Enforcing roles, policies, and standards ensures consistent and cost-effective IT acquisitions and implementations. E-government initiatives require that the citizens' computing environment be included in order to ensure connectivity to all citizens. Decision-making criteria are required in order to ensure that when two divergent technology solutions are possible, some guidelines are provided to prevent internal competing technologies.

Well-defined roles provide clarity in purchasing and deployment objectives and contribute to strong Quality Assurance control points. Standards provide efficiency in costs, including purchase power, standardized training programs, and focused staff recruiting efforts. It lessens the complexity of systems management and administration.

Principles

In order to ensure stable technology, agencies should purchase platforms and operating systems that are tested and accepted by the IT industry.

Long-term IT plans should include strategies for long-term technology migration, including removal of obsolete technology as well as the implementation and move to the new technologies.

Agencies should have a platform replacement policy.

Operating systems will be compliant with POSIX, XPG4 and UNIX 95 branding.

Hardware vendors will be ISO9002 compliant.

Storage subsystems will be compliant with industry standards, and will be platform-independent.

Hardware and software should comply with industry standards for remote control and monitoring.

Application configuration decisions should be based on N-tiered technology.

Standards

NIST FIPS PUB 189 (POSIX.2)
NIST FIPS PUB 151-2 (POSIX.1)
IEEE 1003.1c: 1994

Technologies

Hardware:	Pentium I, II, III, 4 Power PC
Operating Systems:	Unix OS400 Windows Linux OS390
Utilities:	Storage Utilities Backup

Category	Emerging Standard	Current Standard	Twilight Standard
Hand-held Computers	Pocket PC	Palm Pilot HPC	
Laptop Workstations		Power PC Pentium II, III or Celeron	16 bit OS Intel x486 or lower
Thin Client/Terminal	Java VM	Citrix/Winframe	3270 VTxxx 3270 Emulation
Fat PC Client	LINUX	Windows 95 - 98 Power PC NT 4.0 WIN 2000 PRO	DOS 16 Bit OS Win 3.x OS/2 NT 3.51
High End Desktop Workstation	WIN 2000 PRO	Sun Solaris PowerPC	
Workgroup NOS Server	WIN 2000 PRO	NetWare 5.x or 4.x Citrix/NT	NetWare 3.x NT 3.51
Small Server	LINUX 64 bit OS	Intel Pentium III Alpha, DEC UNIX HP, HP/UX IBM RS6000, AIX AS400	Intel 80386/80486 VAX/VMS SCO OS/2
Medium Server	Sparc Ultra Clustered NT \ WIN 2000 Server LINUX 64 bit OS	Intel Pentium III Sparc/Solaris Alpha, DEC UNIX HP, HP/UX IBM RS6000, AIX AS400	Intel 80386/80486 VAX/VMS
Large Server	Sparc E-class Clustered NT 64 bit OS	Alpha, DEC UNIX HP, HP/UX IBM RS6000, AIX AS400	VAX/VMS
Enterprise Server	Sparc HPC	OS/390	VAX/VMS

Category	Emerging Standard	Current Std	Twilight Standard
Printers		HP LaserJet Color Laser Color Ink Jet	Dot Matrix Other impact
Peripherals	Desktop Video		
Management		Novell ManageWise MS SMS UniCenter TNG Tivoli	CMIP
Subsystems		Automatic Tape Library DLT 8mm SAN	4mm 9 track 4250
Disk Subsystem		SCSI hub Optical Laser Disc SAN	
CTI Systems			
VRU			
Scanners		TWAIN	
Desktop Video		See section 4.8	

Technology Trend 1 - The performance of computer hardware will continue to grow exponentially, while costs continue to decline dramatically (Moore's Law).

- "Chip performance doubles, prices halve, in a 12-18 month lifecycle"
- Moore's Law valid for at least another 10 years
- Scope has grown to include almost all computer technology
- Examples: CPU/MIPS, RAM, Disk Storage, etc.

Technology Trend 2 - Microsoft and Intel will dominate business computing.

- It's not about superior technology, it's about market forces
- If better technology appears, it can be bought, cloned or buried
- Impacts Desktop, Client OS, Server OS, Network OS, Thin Client
- Consolidation of UNIX to 3 vendors, server-side only
- Rapidly diminishing emphasis of Mainframes

Privacy Domain

Description

The Privacy domain addresses the privacy concerns of citizens and agencies with well-defined roles, policies, procedures, and technologies. In addition, the Privacy domain addresses all state and federal laws related to privacy issues such as the distribution, availability, notification or permission to distribute, and privacy violation notification. The Privacy domain focuses on the unauthorized viewing and/or acquisition of information about a person, case, or other classified activity.

Purpose

The Privacy domain addresses privacy issues associated with system utilization and information access. It focuses on user and access management but does not include items addressed in the Security Domain (i.e. theft and vandalism). At one time or another the Privacy domain has relationships with all domains with respect to privacy issues, but does not include platforms, operating systems, communications infrastructure components, resident applications, middleware, or databases. The Platform Architecture, Application Engineering Architecture, Middleware Architecture, Network Architecture, and Database domains need to be referenced for guidance on the aspects associated with implementation of these technologies.

Internet access has had a two-fold impact on privacy. One, more citizens and agencies are directly connected to a common worldwide network with immature features for controlling unauthorized access to confidential data and information. Two, Internet access has prompted the mandated sharing of data and information (often regulatory mandates) over the Internet. Data and information transport is vulnerable to unauthorized interception and immature encryption and certification technologies. E-government concepts require sharing of information between agencies that was either duplicated or not provided in the past.

The Privacy domain provides the rigor needed to protect confidential data as well as raise the awareness of potential vulnerabilities, allowing parties to make conscious decisions about transporting private information via digital means. It ensures compliance with federal and state privacy laws and generates user confidence with respect to confidentiality.

Principles

- ❑ Agencies should support strong encryption
- ❑ Privacy protection should be a design goal incorporated into any software that could entail an interaction between a user and a system or network that others have access to.
- ❑ Investigations online must be narrowly tailored to accomplish an explicit, legitimate government purpose.
- ❑ Provide consumers and employees with easily understood information about policies regarding the collection, use, and disclosure of personal data.
- ❑ Limit the collection and use of personal data to that which is needed for valid government purpose.
- ❑ Universal standards should be adopted that define privacy rights and the technical and legal means of securing them.

- ❑ Maintain the accuracy of the personal data held, including establishing, as appropriate, mechanisms allowing consumers and employees to have the opportunity to review and correct their personal data.
- ❑ Furnish consumers and employees with information on the intended use of personal data, and with mechanisms permitting the exercise of choice on its disclosure. More specifically,
- ❑ If personal data is provided to an affiliated third party, the third party will be required to adhere to similar data protection principles that provide for keeping such data confidential.
- ❑ Take appropriate steps to ensure that personal data is protected from unauthorized access and disclosure, including limiting access to such data only to those employees with a business need to know.
- ❑ Apply these principles via practices that have the equivalent effect regardless of the specific technologies employed for data collection and use.
- ❑ The public or employees should have a reasonably consistent expectation of privacy in both electronic and paper-based environments.

Standards

HIPPHA

FERPA (students),

CFA (patients)

Technologies

Security Domain

Description

The Security domain defines the roles, technologies, standards, and policies necessary to protect the information assets of states and their citizenry from vandalism, theft, and any other form of unauthorized access. The Security domain defines the security and access management principles that are applied to ensure the appropriate level of protection for states' information assets. This domain facilitates identification, authentication, authorization, administration, audit, and naming services.

Some examples of subject areas include but are not limited to:

Single sign on
Encryption
Access Control

Some examples of technology components include but are not limited to:

User Ids
Proprietary tokens
Biometrics
Smart Cards/ Card readers

Purpose

The Security domain standardizes the methodology, approach, and technology components utilized in the implementation of information resource protection measures. The domain is associated with virtually all other architecture because security needs must be assessed and applied where necessary in all phases of information resource development and management. The Security domain does not include the privacy aspects associated with deployment of information technologies.

Government, industry, and the public are realizing numerous benefits from the emergence of new information technologies and the increased availability of the Internet. This technology boom has also increased the security risk to the state's information resources. With the ever-increasing percentage of the public that is Internet capable, there has also been an increase in the number of Internet users with malicious intent as well as an increase in the availability of malicious tools and viruses. Decision-making criteria are required in order to ensure that security requirements are identified and security components are incorporated to provide the appropriate level of protection for the government entity's information resources.

Security policies need to provide consistency across the enterprise, and appropriate measures need to be in place to support authorized exchange of information between systems of different security levels. Security involves many aspects, such as providing:

- Physical security of the data and resources used to produce the data.
- Protection against unauthorized and inappropriate use that could potentially impede authorized and appropriate use of the resource.
- Identification and validation of the person who is requesting the information
- Control of access involves the ability to read, write, delete or otherwise acquire access to information.

- Data Privacy or confidentiality includes protection of information from unauthorized disclosure and interception.
- Data integrity or protecting the data from unauthorized modification, including unintentional modifications caused by disk errors, system problems, etc.
- Audit trails for accountability.
- Non-repudiation involves proving either the validity of the data and/or the occurrence of actions with respect to the origin of data (or transaction) and the delivery (or receipt) of the data.

Principles

NIST provides a comprehensive list of 33 principles governing security:

1. Establish a sound security policy as the "foundation" for design.
2. Treat security as an integral part of the overall system design.
3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
4. Reduce risk to an acceptable level
5. Assume that external systems are insecure.
6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
7. Implement layered security (Ensure no single point of vulnerability).
8. Implement tailored system security measures to meet organizational security goals.
9. Strive for simplicity.
10. Design and operate an IT system to limit vulnerability and to be resilient in response.
11. Minimize the system elements to be trusted.
12. Implement security through a combination of measures distributed physically and logically.
13. Provide assurance that the system is, and continues to be, resilient in the face of expected threats
14. Limit or contain vulnerabilities.
15. Formulate security measures to address multiple overlapping information domains.
16. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
17. Use boundary mechanisms to separate computing systems and network infrastructures.
18. Where possible, base security on open standards for portability and interoperability.
19. Use common language in developing security requirements.
20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
23. Use unique identities to ensure accountability.
24. Implement least privilege.
25. Do not implement unnecessary security mechanisms.
26. Protect information while being processed, in transit, and in storage.
27. Strive for operational ease of use.
28. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
29. Consider custom products to achieve adequate security.
30. Ensure proper security in the shutdown or disposal of a system.
31. Protect against all likely classes of "attacks."
32. Identify and prevent common errors and vulnerabilities.
33. Ensure that developers are trained in how to develop secure software.

Standards

- NIST FIPS PUB 112 (Password Usage) Architectures and applications Operating system security
- NIST FIPS PUB 113 (Computer Data Authentication) Authentication
- NIST FIPS PUB 140-1 (Security Requirements for Cryptographic Modules) Confidentiality - Data encryption security
- NIST FIPS PUB 185 (EES) Confidentiality - Data encryption security
- NIST FIPS PUB 46-2 (DES) Confidentiality - Data encryption security
- NIST FIPS PUB 74 (Guidelines for DES) Confidentiality - Data encryption security
- NIST FIPS PUB 81 (DES Modes of Operation) Confidentiality - Data encryption security
- PL 100-235 (Computer Security Act of 1987) Confidentiality - Open systems confidentiality
- PL 93-579 (Privacy Act of 1974) Confidentiality - Open systems confidentiality
- FIPS PUB (DSS)* DRAFT Digital Signature
- IEEE 1003.1b:1993 (POSIX Real-Time Extensions) System management security - Security Management
- NIST FIPS PUB 151-2 (POSIX.1) System management security - Security management
- NIST FIPS PUB 191 (Guideline for LAN Security)
- Computer Security Act of 1987 (Public Law 100-235)
- Computer Fraud and Abuse Act of 1986 (Public Law 99-474)
- Freedom of Information Act of 1980 (Public Law 93-502)
- Financial Integrity Act of 1982 (Public Law 97-225)

- Electronic Communications Privacy Act of 1986 (Public Law 99-508)
- Privacy Act of 1974 (Public Law 93-5790, 5 United States Code 552a, July 14, 1987)
- Executive Order 10450 of April 27, 1954
- Federal Personnel Manual (FPM), Chapter 736-13, 1988
- Copyright Act (17 United States Code 105)
- U.S. Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, February 8, 1996
- OMB Circular A-123, Management Accountability & Control, June 21, 1995
- OMB Circular A-127, Financial Management Systems, July 30, 1993
- OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information, July 9, 1990.
- Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) Special Publications

Telecommunications Standards

- International Organization for Standardization (ISO) - Open Systems Interconnection (OSI) Reference Model (ISO/DIS 7498)
- FIPS 146-2, TCP/IP for wide-area network transmission.
- RFC 791 as the definition of IP for wide area network transmission.
- Border Gateway Protocol, BGP, as defined by RFC 1771 is the protocol for the demarcation points.
- Local Area Networks (LAN) Ethernet II, IEEE 802.3, or IEEE 802.xx (100mbps).

Technologies

Industry Trend 1- The introduction of new technologies also tends to introduce new areas of vulnerability to once secure systems. New security technologies tend to lag behind these introductions. All individuals and organizations would do well to follow the following recommendations from Fred Avolio and Marcus Ranum, in their article written for *Network Magazine*, July 1999.

- Minimalism: Simple is better than complex. There are two basic paradigms: That which is not expressly prohibited is permitted. That which is not expressly permitted is prohibited. Minimalism supports the second paradigm.
- Reductionism: Simplicity is important. Security and complexity are often inversely proportional.
- Restriction: The ideal number of users would be zero, since someone compromising a user account causes nearly all security breaches.
- Accountability: User identification is vital.
- Auditabilty: Gather as much information as possible; it is easier to sift through the information later if needed.

- Configurability: A security device is one of the methods used to implement a security policy. A security policy is based on input from a risk assessment and a business-needs analysis. A security device should not impose roles of its own, but be flexible to change as policy changes.
- Examinability: The methods and algorithms used to implement security should be implemented transparently.

Industry Trends 2 - "Intelligence"-oriented technologies are becoming increasingly available from commercial vendors.

- DW, KM, GIS, Imagery, Analysis Tools, Language Translation, Agents, targeted news services, etc.
- Explosion in commercial information security tools and methods
- Impact on Buy vs. Build decision

State Branding Domain

Description

User interface services define how users interact with an application on local or remote systems. A graphical user interface (GUI) attempts to provide a consistent "look and feel" through the use of a “window manager" which is designed to be operationally consistent. The GUI consists of graphical objects such as windows, menus, icons, and pointers, which allow users to access and use data, graphical images, and applications. The following environments provide user interface services

Purpose

Principles

- ❑ User interfaces will be consistent and user-friendly across all state systems.
- ❑ Interfaces should be well-organized, with a consistent look and feel.
- ❑ Web pages should be designed such that everything can fit on a single page; users typically do not like to scroll.
- ❑ Interfaces should be intuitive and self explanatory.
- ❑ Invest in usability engineering for help in designing workable web pages.
- ❑ For security purposes, it is desirable to have separate visual identities for internal and external web pages (making it clear to users and authors when information could be accessed by outsiders).

Standards

NIST FIPS PUB 158-1 (X-Windows) GUI Client-Server Operations - Data interchange format for GUI- based applications.

Technologies

AAMVA	American Association of Motor Vehicle Administrators
APHSA	American Public Human Services Association
CEG	Center for Economic Growth
COVETS	Commonwealth of Virginia Information Technology Symposium(**COVITS**)
CSG	Council of State Governments
CTG	Center for Technology
FIPS	Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions. See background information for more details.
Global	
JDBC	JDBC™ technology is an API that lets you access virtually any tabular data source from the Java™ programming language. It provides cross-DBMS connectivity to a wide range of SQL databases, and now, with the new JDBC API, it also provides access to other tabular data sources, such as spreadsheets or flat files.
MetaMatrix: MetaBase	The key to managing data is managing metadata. **MetaBase** is an enterprise-caliber metadata management system. MetaBase helps organizations uncover, understand, and share the information resources in the enterprise. MetaBase lets organizations model enterprise information resources into integrated models, or "virtual databases," to streamline the application development process.
MOF	Meta Object Facility (MOF) enables all metamodels and models to be defined in a single "language," and since it is a single

	language, there are no walls preventing the capture of cross-model relationships. MOF is an extremely powerful modeling language that can define many meta-models (relational, object, XML Schema, XML documents, UML, business processes, workflow, etc). OMG has defined many "standard" metamodels, UML, CWM, ect, but the real power of MOF is the ability to define any special purpose metamodel required to facilitate a Model Driven Architecture.
NAGARA	National Association of Government Archives and Records Administrators
NAPA	
NARUC	National Association of Regulatory Utility Commissioners
NASBO	National Association of State Budget Officers
NASCA	National Association of State Chief Administrators
NASPE	
NASPO	National Association of State Procurement Officials
NASTD	**National Association of State Telecommunications Directors**
NCSBCS	National Conference of States on Building Codes and Standards.
NCSC	
NECCC	National Electronic Commerce Coordinating Council Home Page
NIST – National Institute for Standards and Technology	Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs: • the NIST Laboratories, conducting research that advances the nation's technology infrastructure and is needed by U.S. industry to continually improve products and services; • the Baldrige National Quality Program, which promotes performance excellence among U.S. manufacturers, service companies, educational

	institutions, and health care providers; conducts outreach programs and manages the annual Malcolm Baldrige National Quality Award which recognizes performance excellence and quality achievement; • the Manufacturing Extension Partnership, a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and • the Advanced Technology Program, which accelerates the development of innovative technologies for broad national benefit by co-funding R&D partnerships with the private sector.
NSAA	
ODBC	Open Database Connectivity (ODBC) is a widely accepted application programming interface (API) for database access. It is based on the Call-Level Interface (CLI) specifications from X/Open and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language.
Performance Based Budgeting	What constitutes performance varies to some extent from state to state. Typically, this variation involves different specifications of the type of performance information that is required by the law. Terms such as input, process, output, outcome, effectiveness and efficiency are used in the context of performance measurement across the states.
PSWIN	
SOAP	Simple Object Access Protocol SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for

	representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; All SOAP messages are encoded using XML
UDDI	The Universal Description, Discovery and Integration (UDDI) protocol is one of the major building blocks required for successful Web services. UDDI creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use Web services over the Internet. UDDI also allows operational registries to be maintained for different purposes in different contexts. UDDI is a cross-industry effort driven by major platform and software providers, as well as marketplace operators and e-business leaders within the OASIS standards consortium. http://www.uddi.org/.
UETA	UNIFORM ELECTRONIC TRANSACTIONS ACT (**UETA**)
WSDL	Web Services Description Language WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP

	GET/POST, and MIME. As communications protocols and message formats are standardized in the web community, it becomes increasingly possible and important to be able to describe the communications in some structured way. WSDL addresses this need by defining an XML grammar for describing network services as collections of communication endpoints capable of exchanging messages. WSDL service definitions provide documentation for distributed systems and serve as a recipe for automating the details involved in applications communication. A WSDL document defines **services** as collections of network endpoints, or **ports**. In WSDL, the abstract definition of endpoints and messages is separated from their concrete network deployment or data format bindings. This allows the reuse of abstract definitions: **messages**, which are abstract descriptions of the data being exchanged, and **port types** which are abstract collections of **operations**. The concrete protocol and data format specifications for a particular port type constitutes a reusable **binding**. A port is defined by associating a network address with a reusable binding, and a collection of ports define a service. Hence, a WSDL document uses the following elements in the definition of network services: **Types**– a container for data type definitions using some type system (such as XSD). **Message**– an abstract, typed definition of the data being communicated.

	Operation– an abstract description of an action supported by the service. **Port Type**–an abstract set of operations supported by one or more endpoints. **Binding**– a concrete protocol and data format specification for a particular port type. **Port**– a single endpoint defined as a combination of a binding and a network address. **Service**– a collection of related endpoints.
Zero-Based Budgeting	The objective of Zero Based Budgeting is to "reset the clock" each year. While a traditional budgeting process allows managers to start with last year's expenditures and add a percent for inflation to come up with next year's budget, Zero Based Budgeting implies that managers need to build a budget from the ground up, building a case for their spending as if no baseline existed -- to start at zero.
ERISA	US Department of Labor on the Employee Retirement Income Security Act (**ERISA**)